Bull. Aust. Math. Soc. **106** (2022), 1–6
doi:10.1017/S0004972722000247

A NEW CHARACTERISATION FOR QUARTIC RESIDUACITY OF 2

CHAO HUANG and HAO PAN

(Received 6 September 2021; accepted 14 January 2022; first published online 14 March 2022)

Abstract

Let p be a prime with $p \equiv 1 \pmod 4$. Gauss first proved that 2 is a quartic residue modulo p if and only if $p = x^2 + 64y^2$ for some $x, y \in \mathbb{Z}$ and various expressions for the quartic residue symbol $(\frac{2}{p})_4$ are known. We give a new characterisation via a permutation, the sign of which is determined by $(\frac{2}{p})_4$. The permutation is induced by the rule $x \mapsto y - x$ on the $(p-1)/4$ solutions (x, y) to $x^2 + y^2 \equiv 0 \pmod p$ satisfying $1 \le x < y \le (p-1)/2$.

2020 *Mathematics subject classification*: primary 11A15; secondary 05A05, 11A07.

Keywords and phrases: quartic residue, permutation, class number.

1. Introduction

For an odd prime p, an integer a with $(a, p) = 1$ is called a quartic or biquadratic residue modulo p provided $x^4 \equiv a \pmod p$ is solvable. Clearly a is a quartic residue if and only if $a^{(p-1)/4} \equiv 1 \pmod p$. We need only consider $p \equiv 1 \pmod 4$, since for $p \equiv 3 \pmod 4$, the quartic residues coincide with quadratic residues.

Concerning quartic residuacity of 2 modulo p, we may further assume $p = 8n + 1$ so that $(\frac{2}{p}) = 1$. Then the quartic residue symbol $(\frac{2}{p})_4 = \pm 1$ is determined by the congruence $(\frac{2}{p})_4 \equiv 2^{(p-1)/4} \pmod p$.

It was observed by Euler and first proved by Gauss [5] via the law of quartic reciprocity (see [2, 7]) that

$$\left(\frac{2}{p}\right)_4 = 1 \iff p = x^2 + 64y^2 \quad \text{for some } x, y \in \mathbb{Z}.$$

Barrucand and Cohn [1] proved several more equivalences:

$$(-1)^n\left(\frac{2}{p}\right)_4 = 1 \iff \left(\frac{1+\sqrt{2}}{p}\right) = 1 \iff (-1)^{h(-4p)/4} = 1$$
$$\iff p = a^2 + 32b^2 \quad \text{for some } a, b \in \mathbb{Z}$$

The first author is supported by the National Natural Science Foundation of China (Grant No.11971222).
The second author is supported by the National Natural Science Foundation of China (Grant No.12071208).

$$\begin{aligned}&\iff p=c^2-32d^2 \quad \text{for some } c,d\in\mathbb{Z} \text{ with } |c|\equiv 1 \pmod 4)\\ &\iff p=e^2+16f^2 \quad \text{with } e,f\in\mathbb{Z} \text{ and } (-1)^{(e-1)/2}e-1\equiv 4f \pmod 8).\end{aligned} \tag{1.1}$$

Here, $h(-4p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$ and $\sqrt{2}$ denotes any integer x satisfying $x^2 \equiv 2 \pmod p$. (A simple proof for the last three expressions can be found in [10].) Hasse [6] obtained a simple expression via the class number of $\mathbb{Q}(\sqrt{-2p})$:

$$\left(\frac{2}{p}\right)_4 = (-1)^{h(-8p)/4}. \tag{1.2}$$

(Note that (1.2) is related to (1.1) because $h(-4p)+h(-8p)\equiv 4n \pmod 8$ by [9, Proposition 2].) Lehmer [8] modified the argument of Gauss' lemma to prove

$$\left(\frac{2}{p}\right)_4 = 1 \iff \left|\left\{1\le x\le \frac{p-1}{4} : \left(\frac{x}{p}\right)=-1\right\}\right| \equiv 0 \pmod 2.$$

Let $\mathbb{F}_p$ denote the finite field with p elements. The Legendre symbol $(\frac{a}{p})$ can be defined as the sign of the permutation of $\mathbb{F}_p$ sending $x\mapsto ax$ by Zolotarev's theorem (see [3, 4]). Our aim is to find a simple permutation, the sign of which is determined by the quartic residuacity of 2 modulo p.

Assume $p\equiv 1 \pmod 4$ from now on. For such primes, there are nontrivial solutions to $x^2+y^2\equiv 0 \pmod p$ in $\mathbb{F}_p^*$. Moreover, for any x with $1\le x\le (p-1)/2$, there exists a unique y with $1\le y\le (p-1)/2$ such that (x,y) is a solution. So there are $(p-1)/4$ essentially different solutions. For example, for $p=29$, we need only consider seven pairs (x,y) with $1\le x<y\le (p-1)/2$:

$$(1,12),\ (2,5),\ (3,7),\ (4,10),\ (6,14),\ (8,9),\ (11,13). \tag{1.3}$$

Observe that the difference of the two numbers in any pair always gives the first component of another pair, that is, $12-1=11$, $13-11=2$, $5-2=3$ and so on. This observation leads to the following theorem.

THEOREM 1.1. *Let p be a prime with $p\equiv 1 \pmod 4$. Set*

$$A := \{(a,\tilde a)\in\mathbb{Z}\times\mathbb{Z} : a^2+\tilde a^2\equiv 0 \pmod p),\quad 1\le a<\tilde a\le (p-1)/2\}. \tag{1.4}$$

Then we can define a permutation ψ_p of A by the rule $a\mapsto \tilde a - a$ applied to the first component.

The theorem implies

$$\sum_{(a,\tilde a)\in A} a = \sum_{(a,\tilde a)\in A} (\tilde a - a) = \frac{1}{2}\sum_{(a,\tilde a)\in A} \tilde a.$$

However, $\{1,2,\ldots,(p-1)/2\}$ is partitioned into $(p-1)/4$ pairs in A. Thus

$$\sum_{(a,\tilde a)\in A} (a+\tilde a) = \sum_{x=1}^{(p-1)/2} x = \frac{p^2-1}{8}.$$

Thus we immediately obtain the next corollary.

https://doi.org/10.1017/S0004972722000247 Published online by Cambridge University Press

COROLLARY 1.2. *We have*

$$\sum_{(a,\tilde{a})\in A} a = \frac{p^2-1}{24} \quad \textit{and} \quad \sum_{(a,\tilde{a})\in A} \tilde{a} = \frac{p^2-1}{12}.$$

We now study the sign of ψ_p. Let $\{x\}_p$ as usual denote the least nonnegative residue of x modulo p. Set $i = \{\prod_{x=1}^{(p-1)/2} x\}_p$ so that $i^2 \equiv -1 \pmod p$ by Wilson's theorem.

We define $\mathcal{U}_4 = \{\pm 1, \pm i\}$. Then $\mathbb{F}_p^*/\mathcal{U}_4$ is a cyclic group of order $(p-1)/4$ and multiplication by $i-1$ induces a permutation Ψ_p of this quotient group. As an example, for $p = 29$ again, $i = \{14!\}_{29} = 12$. Thus Ψ_{29} is obtained from multiplication by 11 and can be illustrated by its action on cosets as follows:

$$\hookrightarrow \begin{Bmatrix}1\\12\\17\\28\end{Bmatrix} \mapsto \begin{Bmatrix}11\\13\\16\\18\end{Bmatrix} \mapsto \begin{Bmatrix}2\\5\\24\\27\end{Bmatrix} \mapsto \begin{Bmatrix}3\\7\\22\\26\end{Bmatrix} \mapsto \begin{Bmatrix}4\\10\\19\\25\end{Bmatrix} \mapsto \begin{Bmatrix}6\\14\\15\\23\end{Bmatrix} \mapsto \begin{Bmatrix}8\\9\\20\\21\end{Bmatrix} \mapsto$$

Comparing this with (1.3), we see that the permutation ψ_p shows the behaviour of certain representatives in the cosets under Ψ_p. This is because for any pair $(a, \tilde{a}) \in A$, we have $\tilde{a} = \pm ia \pmod p$. Hence the rule of ψ_p can be considered as $a \mapsto \{\pm(\pm i - 1)a\}_p$. However, all the four possibilities $\pm(i \pm 1)$ are in the same coset in $\mathbb{F}_p^*/\mathcal{U}_4$, which implies that ψ_p induces Ψ_p in the quotient group. Hence they have the same sign.

THEOREM 1.3. *For a prime $p \equiv 1 \pmod 4$, define $i = \{\prod_{x=1}^{(p-1)/2} x\}_p$ and $\mathcal{U}_4 = \{\pm 1, \pm i\}$. Then the sign of ψ_p in Theorem 1.1 is equal to that of Ψ_p, the permutation of $\mathbb{F}_p^*/\mathcal{U}_4$ induced by $x \mapsto (i-1)x$. Further*

$$\operatorname{sign}(\psi_p) = \operatorname{sign}(\Psi_p) = \begin{cases} (-1)^n \left(\dfrac{2}{p}\right)_4 & \textit{if } p = 8n+1, \\ 1 & \textit{if } p = 8n+5. \end{cases}$$

In other words, ψ_p is an odd permutation only in two cases:

(i) $p \equiv 1 \pmod{16}$ and 2 is a quartic nonresidue modulo p;
(ii) $p \equiv 9 \pmod{16}$ and 2 is a quartic residue modulo p.

Now consider the mapping $\tilde{a} \mapsto a + \tilde{a}$. As in the argument before Theorem 1.3, it induces the same permutation Ψ_p. In view of Theorem 1.1, $(a, \tilde{a})$ is sent by ψ_p to either $(\tilde{a} - a,\ a + \tilde{a})$ or $(\tilde{a} - a,\ p - (a + \tilde{a}))$, depending on which one belongs to A. This gives the next corollary.

COROLLARY 1.4. *For an integer x, determine $\|x\|_p$ as the unique integer such that $0 \le \|x\|_p < p/2$ and $\|x\|_p \equiv \pm x \pmod p$. Then the permutation ψ_p of A sends $\tilde{a}$ to $\|a + \tilde{a}\|_p$ applied to the second component.*

Theorems 1.1 and 1.3 will be proved in the next two sections, respectively.

https://doi.org/10.1017/S0004972722000247 Published online by Cambridge University Press

2. Proof of Theorem 1.1

Let i be defined as in Theorem 1.3 so that $i^2 \equiv -1 \pmod p$ and let $\|x\|_p$ be as in Corollary 1.4. Clearly $\|x\|_p = \|-x\|_p$ and $\|xy\|_p = \|\,\|x\|_p y\,\|_p$. Define

$$\mathcal{V}_p := \Big\{1 \le x \le \frac{p-1}{2} : x < \|ix\|_p\Big\}.$$

Clearly $|\mathcal{V}_p| = (p-1)/4$. For each $a \in \{1, \dots, (p-1)/2\}$, we set $\tilde{a} := \|ia\|_p$. In view of the definition of A in (1.4), we have $\{(a, \tilde{a}) : a \in \mathcal{V}_p\} = A$.

For convenience, we use the same ψ_p for the mapping $a \mapsto \tilde{a} - a$ with domain $\mathcal{V}_p$. It suffices to prove that ψ_p is a permutation of $\mathcal{V}_p$. First we show that $\psi_p(\mathcal{V}_p) \subseteq \mathcal{V}_p$. As $\tilde{a} = \|ia\|_p$, we partition $\mathcal{V}_p$ into $V_1 \cup V_2$, where

$$V_1 := \{a \in \mathcal{V}_p : \tilde{a} = \{ia\}_p\} \quad \text{and} \quad V_2 := \{a \in \mathcal{V}_p : \tilde{a} = p - \{ia\}_p\}.$$

For $a \in V_1$, we have $a < \tilde{a} = \{ia\}_p \le (p-1)/2$ and hence

$$\psi_p(a) = \{ia\}_p - a = \{(i-1)a\}_p.$$

Furthermore, as $i^2 \equiv -1 \pmod p$,

$$\|i\psi_p(a)\|_p = \|i(i-1)a)\|_p = \|(i+1)a\|_p.$$

To show $\psi_p(a) \in \mathcal{V}_p$, we need to verify

$$\{(i-1)a\}_p < \|(i+1)a\|_p. \tag{2.1}$$

If $\{(i+1)a\}_p > p/2$, then

$$\{(i-1)a\}_p < \{ia\}_p = \tilde{a} < \{(i+1)a\}_p.$$

Thus

$$\{(i+1)a\}_p + \{(i-1)a\}_p = 2\{ia\}_p = 2\tilde{a} < p.$$

Then (2.1) holds since

$$\|(i+1)a\|_p = p - \{(i+1)a\}_p > \{(i-1)a\}_p.$$

If $\{(i+1)a\}_p < p/2$, then (2.1) is also true since

$$\|(i+1)a\|_p = \{(i+1)a\}_p = \{2a + (i-1)a\}_p = 2a + \{(i-1)a\}_p > \{(i-1)a\}_p.$$

Therefore, $\psi_p(V_1) \subseteq \mathcal{V}_p$. Using a similar argument, $\psi_p(V_2) \subseteq \mathcal{V}_p$. Thus it suffices to show that ψ_p is an injection to prove the theorem.

Assume, on the contrary, there exist distinct $a_1, a_2 \in \mathcal{V}_p$ such that $\psi_p(a_1) = \psi_p(a_2)$. If $a_1, a_2 \in V_1$, then $a_1 \not\equiv a_2 \pmod p$ and $\{(i-1)a_1\}_p = \{(i-1)a_2\}_p$, which is evidently impossible. Similarly, $a_1, a_2 \in V_2$ is impossible. So we may assume that $a_1 \in V_1$ and $a_2 \in V_2$, that is, $\tilde{a}_1 \equiv ia_1 \pmod p$ and $\tilde{a}_2 \equiv -ia_2 \pmod p$. Then

$$(i-1)a_1 \equiv \psi_p(a_1) = \psi_p(a_2) \equiv (-i-1)a_2 \equiv i(i-1)a_2 \pmod p.$$

https://doi.org/10.1017/S0004972722000247 Published online by Cambridge University Press

It follows that

$$a_1 \equiv i a_2 \equiv -\tilde{a}_2 \pmod{p},$$

which contradicts the fact that $1 \le a_1, \tilde{a}_2 \le (p-1)/2$.

Thus ψ_p is an injection and the proof is complete.

3. Proof of Theorem 1.3

Since $\mathbb{F}_p^*$ is cyclic, $\mathbb{F}_p^*/\mathcal{U}_4$ is also a cyclic group and of order $(p-1)/4$. Let the order of the coset of $1+i$ be m. Then Ψ_p is composed of $(p-1)/4m$ disjoint cycles of length m. Thus

$$\text{sign}\,(\psi_p) = (-1)^{(m-1)(p-1)/4m}. \tag{3.1}$$

Now we divide the discussion into five cases.

Case (i): $p \equiv 1 \pmod{16}$ and 2 is a quartic residue modulo p.

Case (ii): $p \equiv 9 \pmod{16}$ and 2 is a quartic nonresidue modulo p.

In these two cases,

$$[(1+i)^{(p-1)/8}]^4 \equiv (-4)^{(p-1)/8} \equiv (-1)^{(p-1)/8} 2^{(p-1)/4} \equiv 1 \pmod{p},$$

which implies $(1+i)^{(p-1)/8} \in \mathcal{U}_4$. Hence $(p-1)/8$ is divisible by m and ψ_p is even from (3.1).

Case (iii): $p \equiv 1 \pmod{16}$ and 2 is a quartic nonresidue modulo p.

Case (iv): $p \equiv 9 \pmod{16}$ and 2 is a quartic residue modulo p.

In these two cases,

$$[(1+i)^{(p-1)/8}]^4 \equiv (-4)^{(p-1)/8} \equiv (-1)^{(p-1)/8} 2^{(p-1)/4} \equiv -1 \pmod{p}.$$

Therefore, $(1+i)^{(p-1)/4} \in \mathcal{U}_4$ while $(1+i)^{(p-1)/8} \notin \mathcal{U}_4$. In other words, m, a factor of $(p-1)/4$, does not divide $(p-1)/8$. So $q = (p-1)/4m$ must be odd while m is even. Thus ψ_p is odd from (3.1).

Case (v): $p \equiv 5 \pmod{8}$. Now m must be odd since it divides $(p-1)/4$ from the definition. Thus sign $\psi_p = 1$ in view of (3.1). The proof is complete. □

Acknowledgements

We are deeply grateful to the anonymous referee, whose valuable suggestions enabled us to simplify our proof substantially. We would also like to thank Professor Zhi-Wei Sun for his guidance.

https://doi.org/10.1017/S0004972722000247 Published online by Cambridge University Press

References

[1] P. Barrucand and H. Cohn, 'Note on primes of type $x^2 + 32y^2$, class number and residuacity', *J. reine angew. Math.* **238** (1969), 67–70.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (Wiley, New York, 1998).

[3] J. H. Conway, *The Sensual (Quadratic) Form*, Carus Mathematical Monographs, 26 (The Mathematical Association of America, Washington DC, 1997), 127–132.

[4] R. E. Dressler and E. E. Shult, 'A simple proof of the Zolotareff–Frobenius theorem', *Proc. Amer. Math. Soc.* **54** (1976), 53–54.

[5] C. F. Gauss, 'Theoria residuorum biquadraticorum, Commentatio prima', *Comment. Soc. Reg. Gottingensis* 6 (1828), 28 pages. [Collected Works, Volume **2**, 65–92].

[6] H. Hasse, 'Über die Klassenzahl des Körper $P\left(\sqrt{-2p}\right)$ mit einer Primzahl $p \neq 2$', *J. Number Theory* **1** (1969), 231–234.

[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn, Graduate Texts in Mathematics, 84 (Springer, New York, 1990).

[8] E. Lehmer, 'Generalizations of Gauss's lemma', in: *Number Theory and Algebra: Collected papers dedicated to Henry B. Mann, Arnold E. Ross, and Olga Taussky-Todd* (ed. H. Zassenhaus) (Academic Press, New York, 1977), 187–194.

[9] A. Pizer, 'On the 2-part of the class number of imaginary quadratic number fields', *J. Number Theory* **8** (1976), 184–192.

[10] K. S. Williams, 'Note on a result of Barrucand and Cohn', *J. reine angew. Math.* **285** (1976), 218–220.

CHAO HUANG, Department of Mathematics,
Nanjing University, Nanjing 210093, People's Republic of China
e-mail: DG1921004@smail.nju.edu.cn

HAO PAN, School of Applied Mathematics,
Nanjing University of Finance and Economics
Nanjing 210023, PR China
e-mail: haopan79@zoho.com